MINUTES IACR STRATEGIC MEETING AT *EUROCRYPT 2024*

26 MAY 2024

1. Opening Matters

1.1. **Welcome, roll of attendees, identification of proxies.** At 10:42 CET the President opens the meeting and briefly goes around for an introductory round, confirming attendees and establishing who is holding proxies. There are 21 full time attendees.

1.1.1. *Roll of Attendees.*

Attendees (Elected). Michel Abdalla (President 2023-2025); Allison Bishop (Vice President 2023-2025); Brian LaMacchia (Treasurer 2023-2025, *RWC* Steering Committee); Benjamin Wesolowski (Secretary 2023-2025); Anna Lysyanskaya (online, Director 2022-2024); María Naya-Plasencia (Director 2024-2026); Bart Preneel (Director 2023-2025, Program Chair Contact); Francisco Rodríguez-Henríquez (Director 2024-2026); Peter Schwabe (Director 2023-2025, *CHES* Steering Committee); Bo-Yin Yang (Director 2022-2024); Moti Yung (Director 2024-2026, *PKC* Steering Committee);

Attendees (Appointed). Dario Fiore (Eurocrypt 2025 General Chair (2024-2025)); Julia Hesse (online, *Eurocrypt 2024* General Chair (2023-2024)); Bertram Poettering (Membership Secretary 2023-2025);

Attendees (Representatives and Others). Gregor Leander (*FSE* Steering Committee); Kevin McCurley (Database Administrator);

Absentees (Elected). Jian Guo (Director 2022-2024); Shai Halevi (Director 2023-2025);

Absentees (Appointed). Foteini Baldimtsi (Communications Secretary 2023-2025); Tancrède Lepoint (*Crypto 2024* General Chair (2023-2024)); Joseph Liu (Asiacrypt 2025 General Chair (2024-2025)); Vincent Rijmen (Journal of Cryptology Editor-in-Chief 2024-2026); Bimal Roy (*Asiacrypt 2024* General Chair 2023-2024);

Absentees (Representatives and Others). Tal Malkin (*TCC* Steering Committee); Mitsuru Matsui (*Asiacrypt* Steering Committee); Hilarie Orman (Archivist); Tal Rabin (Code-of-conduct Liaison); Yu Yu (Webmaster);

The President rapidly goes through the items of the agenda, and the Board decides on an order.

2. Publication and conference model

Over the past few weeks, a working group has been investigating the publication and conference model. Bishop provides a summary. The primary focus of the discussion is on handling the growth of the community. Bishop reviews the tension between several metrics: total program time, acceptance rate, number of submissions, length of talks, number of tracks...

The working group discussed with Carmela Troncoso how security venues have been handling their growth. For instance, Usenix is adopting a hybrid approach: each paper comes with a video, a 1-minute talk (longer for selected papers), and a poster. Although each component has its merits, this approach significantly increases the authors' workload.

2.1. **The link between papers and talk slots.** A core question is: do we want to break the link between papers and talk slots (or, more generally, presentation slots).

Papers could be published without a presentation slot: for instance, papers published in the *IACR Transactions on Symmetric Cryptology* are invited to present at *FSE*, but that is not mandatory. This would require changing the publication model, since the existing format of *conference proceedings* requires some form of presentation. Alternatively, talk slots could be replaced with another form of presentation, such as posters.

2.2. **Poster sessions.** The working group discussed poster sessions, but no consensus emerged. Hesse, as *Eurocrypt 2024* General Chair, notes that some authors offered to present a poster at Eurocrypt. There would have been attractive spots for a poster session at the venue. Posters could easily be an opt-in option.

The Board debates the pros and cons of posters versus traditional talks. Concerns are raised about the quality and engagement of posters, and their overall impact on the conference experience.

- Arguments against posters: posters provide less exposure for students and young researchers. They radically change the conference experience. They require a process to select which papers get a talk slot, possibly creating two tiers of papers. Such a significant change would be met with resistance.
- In favor of posters: at some point it may become our only option. Shortening talk slots can only go so far; posters are a longer term solution. It simplifies the organisation of the event and the search for appropriate venues. It puts the emphasis on direct interaction between participants, creates social opportunities.
- It is emphasized that, should we take that route, it is important for "poster papers" to remain fully published papers. Conference proceedings would not discriminate papers that were presented as a talk or as a poster. We do not want posters to be perceived as lower-tier.
- To avoid posters being perceived as undesirable lower-tier presentation, the way papers are selected for talks is important. One option is having very few (but longer) talks reserved for a selection of best papers (there would indeed be two tiers, but not much different from the existing Best Paper Awards; a higher number could be awarded, but the proportion would remain small). Another approach is to select talks randomly.

2.3. **Impact on students.** The Board emphasizes the importance of providing adequate exposure for students and considers the implications of decoupling papers from presentations. The following points are raised:

- Giving a talk is an important exercise that benefits younger researchers in several ways (improving their communication skills, giving them exposure...).
- Ideas are discussed to mitigate the impact of reducing the number of talk slots. Students could be given different opportunities, such as a "talk training" workshop or mentorship during the affiliated events; student attendees could then get a slot during a special session of the main event.

2.4. **Acceptance rate.** A general agreement emerges that the acceptance rate should be preserved. As the number of submissions has increased, the proportion of high quality submissions has remained high.

However, it seems that our General Conferences (*Asiacrypt*, *Crypto*, *Eurocrypt*) have absorbed significantly more of the growth than our area conferences (*CHES*, *FSE*, *PKC*, *TCC*). Rather than preserving the acceptance rate per conference, one could aim for an IACR-wide acceptance rate, and rebalance the distribution across conferences.

2.5. **Changing the scale or structure of conferences.** If we want to preserve the acceptance rate, the number of talk slots, and the time allocated per talk, we would need to change the scale or structure of the conferences.

- The most straightforward option is to increase the number of tracks. We have already evolved from one track to three tracks. However, each new track increases both the cost of the conference and the workload of General Chairs. Venues capable of hosting many tracks are rarer and more expensive. Securing a slot at these very large venues is more difficult. It also reduces the number of cities capable of hosting our events.
- It is reminded that the General Chairs are volunteers. If the organisation of our events becomes more complex, we may need professional assistance, which would further increase costs.
- Several ideas to restructure the events are proposed, but none gains much traction: making the event longer (but people do not want longer conferences), using time currently dedicated to affiliated events (but affiliated events are very successful), splitting the week between topics (but the point of general conferences is to get the whole community together).
- LaMacchia highlights the need to consider the financial implications of adding tracks or changing the conference format, particularly regarding registration fees. Increasing registration fees raises accessibility issues.

2.6. **Strategic decision-making.** The Board discusses the decision-making process for handling this issue.

- It is stressed that any significant changes will take several years to implement fully, given the existing plans for upcoming conferences. A venue is chosen two to three years before the event.
- The possibility to let General Chairs (GCs) experiment for solutions is discussed. GCs have some flexibility to experiment, but the Board should ensure continuity by establishing default guidelines. The scalability issue calls for long-term strategic planning.

- Important changes would impact the work of both GCs *and* Program Chairs (PCs). The dynamic between GCs and PCs regarding program structure can be delicate.
- Any experiment requires a commitment of at least two to three years, and the subsequent venues and GCs would be chosen before the conclusion of the experiment.

2.7. **Next steps.** For the next two to three years, small changes (like shortening the talks) should be sufficient. For the direction to take in the long term, we have to consult with IACR members. A panel discussion will be held on Tuesday, with Bishop and McCurley summarizing today's discussion points. The panel concerns both the publication and conference models, while today's discussion focused on the conference model.

Action Point **1:**
Draft guidelines for Program Chairs and General Chairs on how to handle growth for the next three years.

Action Point **2:**
Work on concrete proposals for a long term plan to handle growth to submit to the IACR membership.

3. Staffing and running business

The Treasurer presents the next item on the agenda. With the growth of our events, the IACR has also experienced financial growth. Annual costs and revenue are in the millions of USD. This large organization is entirely run on volunteer efforts. A lot of work falls to General Chairs, but a heavy workload goes back to treasury. There is currently no budget to assist with accounting — neither to cover software costs nor to contract professional services.

McCurley (former Treasurer) stresses that LaMacchia has done an amazing job of improving the processes, and the entire Board thanks him. McCurley suggests that we investigate how organisations of comparable size are handling this issue. Hiring help, possibly a CFO (Chief Financial Officer) could be an option. The Board invites LaMacchia to submit a concrete proposal.

Tied into this, LaMacchia is looking into a future increase in the membership fees. Currently, most of the income from membership fees is allocated to schools and student waivers. The increase would help cover the additional costs of running the organisation.

4. IACR statements

The President introduces the next item on the agenda: should we revise our practice of issuing IACR statements? Matters such as the ongoing situation in Gaza and Israel are delicate to address. These events affect various members of our community, but any public statement is very delicate to craft, and subject to being misconstrued one way or another. It is noted that some associations, like the ACM, have an entire committee dedicated to public policy.

One option would be to adopt a policy that restricts all future IACR statements issued by the Board to topics directly related to our expertise and mission. The Board discusses the pros and cons of such a policy. The main considerations in the discussion are the following:

- Supporting our members everywhere,
- Defending shared humanitarian values,
- Preserving the unity of the IACR community,
- The skill and legitimacy of the Board in geopolitical matters.

It is reminded that statements can always be proposed by IACR members (through a petition signed by 10 percent of the members, followed by a referendum). A policy on statements issued by the Board would not concern statements proposed through this process.

No consensus is reached on how to properly establish a formal policy for statements from the Board. The discussion remains open, and in the meantime, it is advised to avoid further comments on topics outside our domain of expertise. The Board reiterates its strong support to all its members suffering from the consequences of armed conflicts.

5. Requirements for program chairs of general conferences

The President presents the next item on the agenda: should we set minimal requirements for the selection of Program Chairs (PCs) of our General Conferences? Currently, we do not have strict requirements, but we strongly expect the following:

(1) Former experience as a PC (supposedly for smaller events).

(2) Being a prominent and active member of the cryptologic research community (regular publications in IACR conferences, and/or neighboring venues).

5.1. **On Expectation 1.** Given the scale of our General Conferences, there is a consensus that Expectation 1 is crucial. It is noted that being an *Area Chair* (or *Track Chair*) in some large conferences could be regarded as sufficient prior experience. Area Chairs in our General Conferences are selected by PCs. We could mandate that PCs select Area Chairs with the view that they may be good future PC candidates. That would create a pipeline for the selection of PCs.

A discussion begins on the current role of Area Chairs. It is noted that with the growth of our conferences, they play an increasingly important role. This role, however, is not formalized. In particular, there exists no default list of areas to be represented. While PCs have the flexibility to create their own list of areas, a default list could be suggested.

Action Point **3:**
Build a balanced list of areas to be proposed as a default list to Program Chairs.

5.2. **On Expectation 2.** The second expectation serves two purposes. First, as PCs play the most important part in selecting papers and building the program, they must have an intimate understanding of our research community. Second, the respectability of our venues directly relates to the PCs who represent them.

There has never been a minimum bibliometric requirement. Our community is highly diverse, and past Board discussions concluded that strict requirements cannot account for this variety.

The question of looking specifically at IACR publication numbers is brought up. The goal of such a metric would be to ensure that PCs are prominent and active members of the IACR community. In response, it is noted that such a requirement could create or reinforce biases: researchers in the industry or those who publish in multiple neighboring communities may have lower "IACR numbers", but could still make excellent PCs. Some areas are underrepresented in IACR venues, leading some to turn to neighboring communities. For them to feel welcome to IACR venues, they must feel represented in our leadership positions such as PCs.

5.3. **Conclusion.** The majority sentiment of the Board is that Expectation 1 is the most important: candidates should be selected primarily on their capacity to run a Program Committee. Expectation 2 (research activity) remains critical, but it should not be assessed using strict bibliometric criteria. It is decided not to establish formal requirements. The Board is entrusted to select candidates through careful case-by-case considerations.

6. Tasks currently handled by McCurley

McCurley presents the next item on the agenda. He has been handling several tasks for the IACR, some of which are of critical importance. Continuity needs to be ensured when he is no longer handling them. He presents all of these tasks in a few slides, which include the maintenance of the HotCRP fork, operating systems, backups, DNS, mail server, YouTube channel, CryptoDB, and ePrint...

Some of these are complex, like the mail server. The increasing scale and complexity make it unrealistic to keep relying on voluntary work: McCurley advises that the IACR begin relying on professional services. He proposes to draft a job description.

7. Closing Matters

The President closes the meeting officially at 17:46 CET.